

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-126425

(43)Date of publication of application : 11.05.1999

(51)Int.Cl.

G11B 20/10  
G11B 7/00

(21)Application number : 09-292071

(71)Applicant : SONY CORP

(22)Date of filing : 24.10.1997

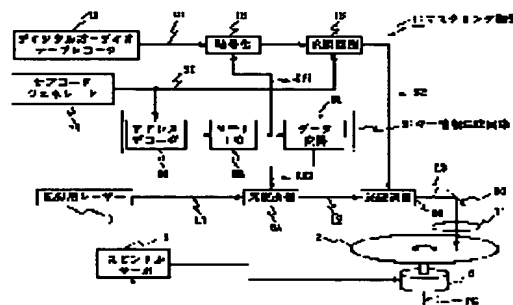
(72)Inventor : KOBAYASHI SEIJI

(54) OPTICAL DISK DEVICE, OPTICAL DISK REPRODUCING METHOD AND OPTICAL DISK

(57)Abstract:

PROBLEM TO BE SOLVED: To make the analysis of encipherment difficult by obtaining a procedure, which is necessary for detecting from an optical disk a key information required for the release of encipherment, from outside an equipment other than the optical disk, and thereby changing the cryptographic method.

SOLUTION: A digital signal processor, after generating a seek command to a servo circuit in response to a user's operation, binarizes with a prescribed threshold value the envelope detection result of a digital reproducing signal DRF obtained from the seek, and reproduces key information KY2. In addition, through a process corresponding to a data conversion circuit 9C at the time of recording, the key information KY2 is parallelly converted to form key information KY1, releasing the encipherment of a digital audio signal reproduced from a compact disk, in accordance with the processing program of a floppy disk supplied with the compact disk in pairs. Then, by the change of various processing procedures, the detection procedure of the key information KY2 is made changeable, as is data processing procedure or the like.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(11)特許出願公開番号

特開平11-126425

(43)公開日 平成11年(1999)5月11日

(51) Int.Cl.<sup>6</sup>

識別記号

FI

G 1 1 B 20/10

7/00

**G 1 1 B 20/10**

7/00

H

R

審査請求 未請求 請求項の数13 O.L (全 10 頁)

(21)出願番号 特願平9-292071

(22)出願日 平成9年(1997)10月24日

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 小林 誠司

東京都品川区北品川6丁目7番35号 ソニ  
一株式会社内

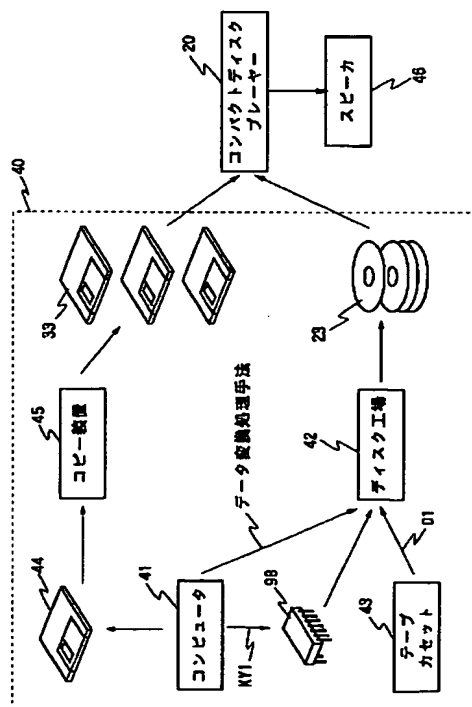
(74)代理人 弁理士 多田 繁範

(54)【発明の名称】 光ディスク装置、光ディスクの再生方法及び光ディスク

(57) 【要約】

【課題】本発明は、光ディスク装置、光ディスクの再生方法及び光ディスクに関し、例えばコンパクトディスクと、その再生装置及び再生方法に適用して、従来に比して一段と確実に違法コピーを防止できるようにする。

【解決手段】暗号化の解除に必要なキー情報を光ディスク23より検出するのに必要な手順を、光ディスク23以外の機器の外部33より取得する。



## 【特許請求の範囲】

【請求項1】 光ディスクにレーザービームを照射して前記光ディスクを再生する光ディスク装置において、前記レーザービームの戻り光に応じて信号レベルが変化する再生信号を生成する再生信号生成手段と、前記再生信号を2値識別して第1のデジタル信号を再生する第1の再生信号処理手段と、所定のキー情報を用いて前記第1のデジタル信号の暗号を解除する暗号処理手段と、前記光ディスクより、前記キー情報の生成に必要な第2のデジタル信号を検出する信号検出手段と、所定の処理手順により、前記第2のデジタル信号より前記キー情報を生成するキー情報生成手段と、前記処理手順を、前記光ディスク以外の機器の外部より取得して前記キー情報生成手段に設定する入力手段とを備えることを特徴とする光ディスク装置。

【請求項2】 前記光ディスクは、ビット又はマークの幅により前記第2のデジタル信号が記録され、前記信号検出手段は、前記再生信号の信号レベルを検出して信号レベル検出結果を出力する信号レベル検出手段と、前記信号レベル検出結果に基づいて、前記第2のデジタル信号を再生する識別手段とを有することを特徴とする請求項1に記載の光ディスク装置。

【請求項3】 前記入力手段は、前記光ディスクとは異なる所定の記録媒体より前記処理手順を取得することを特徴とする請求項1に記載の光ディスク装置。

【請求項4】 前記入力手段は、所定の伝送路を介して前記処理手順を取得することを特徴とする請求項1に記載の光ディスク装置。

【請求項5】 光ディスクにレーザービームを照射して前記光ディスクを再生する光ディスク装置において、前記レーザービームの戻り光に応じて信号レベルが変化する再生信号を生成する再生信号生成手段と、前記再生信号を2値識別して第1のデジタル信号を再生する第1の再生信号処理手段と、所定のキー情報を用いて前記第1のデジタル信号の暗号を解除する暗号処理手段と、前記光ディスクより、前記キー情報の生成に必要な第2のデジタル信号を検出する信号検出手段と、所定の処理手順により、前記第2のデジタル信号より前記キー情報を生成するキー情報生成手段とを備え、前記キー情報生成手段は、前記処理手順が前記光ディスク以外により変更可能に設定されたことを特徴とする光ディスク装置。

【請求項6】 光ディスクにレーザービームを照射して前記光ディスクを再生する光ディスク装置において、前記レーザービームの戻り光に応じて信号レベルが変

する再生信号を生成する再生信号生成手段と、前記再生信号を2値識別して第1のデジタル信号を再生する第1の再生信号処理手段と、所定のキー情報を用いて前記第1のデジタル信号の暗号を解除する暗号処理手段と、所定の検出手順により、前記光ディスクより、前記キー情報の生成に必要な第2のデジタル信号を検出する信号検出手段と、前記第2のデジタル信号より前記キー情報を生成するキー情報生成手段と、前記検出手順を、前記光ディスク以外の機器の外部より取得して前記信号検出手段に設定する入力手段とを備えることを特徴とする光ディスク装置。

【請求項7】 前記光ディスクは、ビット又はマークの幅により前記第2のデジタル信号が記録され、前記信号検出手段は、前記検出手順により指定される箇所より、前記再生信号の信号レベルを検出して信号レベル検出結果を出力する信号レベル検出手段と、前記信号レベル検出結果に基づいて、前記第2のデジタル信号を再生する識別手段とを有することを特徴とする請求項6に記載の光ディスク装置。

【請求項8】 前記入力手段は、前記光ディスクとは異なる所定の記録媒体より前記検出手順を取得することを特徴とする請求項6に記載の光ディスク装置。

【請求項9】 前記入力手段は、所定の伝送路を介して前記検出手順を取得することを特徴とする請求項6に記載の光ディスク装置。

【請求項10】 光ディスクにレーザービームを照射して前記光ディスクを再生する光ディスク装置において、前記レーザービームの戻り光に応じて信号レベルが変化する再生信号を生成する再生信号生成手段と、前記再生信号を2値識別して第1のデジタル信号を再生する第1の再生信号処理手段と、所定のキー情報を用いて前記第1のデジタル信号の暗号を解除する暗号処理手段と、所定の検出手順により、前記光ディスクより、前記キー情報の生成に必要な第2のデジタル信号を検出する信号検出手段と、前記第2のデジタル信号より前記キー情報を生成するキー情報生成手段とを備え、前記信号検出手段は、前記検出手順が前記光ディスク以外により変更可能に設定されたことを特徴とする光ディスク装置。

【請求項11】 光ディスクにレーザービームを照射して得られる戻り光を2値識別して第1のデジタル信号を再生し、所定の処理手順により、前記光ディスクより検出した第

2のデジタル信号よりキー情報を生成し、前記キー情報により前記第1のデジタル信号の暗号化を解除する光ディスクの再生方法であって、前記処理手順を、前記光ディスク以外の機器の外部より取得することを特徴とする光ディスクの再生方法。

【請求項12】光ディスクにレーザービームを照射して得られる戻り光を2値識別して第1のデジタル信号を再生し、

所定の検出手順により前記光ディスクより第2のデジタル信号を検出し、

前記第2のデジタル信号よりキー情報を生成し、前記キー情報により前記第1のデジタル信号の暗号を解除する光ディスクの再生方法であって、前記検出手順を、前記光ディスク以外の機器の外部より取得することを特徴とする光ディスクの再生方法。

【請求項13】所定のキー情報により暗号化された第1のデジタル信号と、所定の処理手順により前記キー情報に変換される第2のデジタル信号とが記録され、前記処理手順が所定の情報伝達手段により伝達されることを特徴とする光ディスク。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、光ディスク装置、光ディスクの再生方法及び光ディスクに関し、例えばコンパクトディスクと、その再生装置及び再生方法に適用することができる。本発明は、暗号化の解除に必要なキー情報を光ディスクより検出するのに必要な手順を、光ディスク以外の機器の外部より取得することにより、従来に比して一段と確実に違法コピーを防止できるようにする。

【0002】

【従来の技術】従来、コンパクトディスクにおいては、リードインエリアの内周側に、製造メーカー、製造場所、ディスク番号等を示す符号が刻印され、この符号を目視確認することにより他のコンパクトディスクと識別できるようになされている。

【0003】

【発明が解決しようとする課題】ところでこの刻印によって記録されるメーカー等の符号は、目視によって認識することを目的とするものである。このため違法コピーを完全には防止できない問題がある。

【0004】このような問題を解決する1つの方法として、ビット幅の変化により識別データを発見困難に記録する方法が考えられる。ところがこのような方法でも、違法コピーの業者に一旦違法コピーの識別方法が判明すると、模倣させる恐れがあり、完全に違法コピーを防止できない問題がある。

【0005】本発明は以上の点を考慮してなされたもので、従来に比して一段と確実に違法コピーを防止することができる光ディスク装置、光ディスクの再生方法及び

光ディスクを提案しようとするものである。

【0006】

【課題を解決するための手段】かかる課題を解決するため本発明においては、光ディスク装置及び光ディスクの再生方法に適用して、光ディスクより検出した第2のデジタル信号よりキー情報を生成する処理手順を、光ディスク以外の機器の外部より取得してキー情報生成手段に設定する。

【0007】また光ディスク装置に適用して、光ディスクより検出した第2のデジタル信号よりキー情報を生成する処理手順を、光ディスク以外により変更可能にする。

【0008】また光ディスク装置及び光ディスクの再生方法に適用して、キー情報の生成に必要な第2のデジタル信号を光ディスクより検出する検出手順を、光ディスク以外の機器の外部より取得して信号検出手段に設定する。

【0009】また光ディスク装置に適用して、キー情報の生成に必要な第2のデジタル信号を光ディスクより検出する検出処理手順を、光ディスク以外により変更可能に設定する。

【0010】また光ディスクに適用して、所定のキー情報により暗号化された第1のデジタル信号と、所定の処理手順によりこのキー情報に変換される第2のデジタル信号とを記録し、先の処理手順が所定の情報伝達手段により伝達されるようにする。

【0011】第2のデジタル信号より所定の処理手順でキー情報を生成し、このキー情報より第1のデジタル信号の暗号化を解除する場合、第2のデジタル信号及び処理手順とが正しい対応関係にあるときだけ、第1のデジタル信号の暗号化を正しく解除することができる。このような関係を前提にして、この処理手順を光ディスク以外の機器の外部より取得してキー情報生成手段に設定すれば、必要に応じてこの処理手順を変更することができる。これにより例えば定期的に、第1のデジタル信号の暗号化、第2のデジタル信号を変更し、この変更に対応するように処理手順を変更して、処理手順、光ディスクを解析して実行される違法コピーを防止することができる。

【0012】またこの処理手順を光ディスク以外により変更可能に設定して、同様に、違法コピーに対応することができる。

【0013】またキー情報の生成に必要な第2のデジタル信号を光ディスクより検出する検出手順を、光ディスク以外の機器の外部より取得して信号検出手段に設定しても、例えば定期的に、第1のデジタル信号の暗号化、第2のデジタル信号を変更し、この変更に対応するように検出手順を変更して、検出手順、光ディスクを解析して実行される違法コピーを防止することができる。

【0014】またキー情報の生成に必要な第2のデジタル信号を光ディスクより検出する検出手順を、変更可能に設定すれば、同様に、違法コピーに対応することができる。

【0015】また光ディスクに適用して、所定のキー情報により暗号化された第1のデジタル信号と、所定の処理手順によりこのキー情報に変換される第2のデジタル信号とを記録するようにし、この処理手順が所定の情報伝達手段により伝達されるようにすれば、同様にして、違法コピーに対応することができる。

【0016】

【発明の実施の形態】以下、適宜図面を参照しながら本発明の実施の形態を詳述する。

【0017】図2は、マスタリング装置を示すブロック図である。この実施の形態においては、必要に応じてこのマスタリング装置が選択され、このマスタリング装置1よりディスク原盤2を順次露光し、コンパクトディスクのマザーディスクを作成する。

【0018】すなわちこのマスタリング装置1において、スピンドルモータ4は、スピンドルサーボ回路5の制御によりディスク原盤2を所定の回転速度で回転駆動する。このときスピンドルモータ4は、底部に取付けられた周波数発電機により、ディスク原盤2が所定角度だけ回転する毎に信号レベルが切り換わるFG信号FGを出力する。

【0019】スピンドルサーボ回路5は、このFG信号FGを基準にして、スピンドルモータ4の回転速度を制御し、いわゆる線速度一定(CLV: Constant Linear Velocity)の条件によりスピンドルモータ4の回転を制御する。

【0020】記録用レーザー7は、例えばガスレーザーにより構成され、レーザービームL1を光変調器8Aに射出する。光変調器8A及び光変調器8Bは、例えば電気音響光学素子により構成される。このうち光変調器8Aは、キー情報生成回路9から供給されるキー情報KY2に従ってレーザービームL1の光量を変化させる。すなわちキー情報KY2の論理レベルが論理1の場合、レーザービームL1を減衰させることなく射出し、キー情報KY2の論理レベルが論理0の場合、レーザービームL1を所定光量だけ減衰させて射出する。

【0021】光変調器8Bは、光変調器8Aより射出されるレーザービームL2をEFM(Eight to Fourteen Modulation)信号S2に応じてオン/オフ制御して射出する。

【0022】ミラー10は、光変調器8Bより射出されるレーザービームL3の光路を折り曲げて、ディスク原盤2に向けて射出する。対物レンズ11は、このミラー10の反射光をディスク原盤2の記録面上に集光する。これらミラー10及び対物レンズ11は、図示しないスレッド機構により、ディスク原盤2の回転に同期して半

径方向に順次移動するようになされ、これによりマスタリング装置1では、ディスク原盤2の内周側から外周側に向かって、ラセン状にトラックを形成し、このトラック上にEFM信号S2に対応したビット形状を形成する。

【0023】さらにこのときレーザービームL1の光量を光変調器8Aにより制御することにより、キー情報KY2に応じてビット幅が変化するようにディスク原盤2を露光し、これによりビット幅の変化によりキー情報KY2を記録する。

【0024】デジタルオーディオテープレコーダ12は、このディスク原盤2に記録するデジタルオーディオ信号D1を出力する。サブコードジェネレータ13は、このデジタルオーディオ信号D1のタイムコード(時、分、秒、フレームにより構成される)を生成する。さらにサブコードジェネレータ13は、このタイムコードより、ディスク原盤2に記録するサブコードデータSCを生成して出力する。なおサブコードジェネレータ13は、リードインエリアに記録するTOCのデータも併せて生成し、対応するタイミングにより出力する。

【0025】キー情報生成回路9は、このサブコードデータSCのタイムコードより、キー情報KY1及びKY2を生成する。すなわちキー情報生成回路9は、アドレスデコーダ9AにサブコードデータSCを入力し、ここでタイムコードをデコードする。メモリIC9Bは、ビット情報を保持するリードオンリメモリ又はEPROMで構成され、タイムコードをアドレスにしてDES(Data Encryption Standard)符号による54ビットのキー情報KY1を出力する。これによりキー情報生成回路9は、デジタルオーディオ信号D1の処理単位であるフレーム毎に、タイムコードに対応するキー情報KY1を出力する。

【0026】データ変換回路9Cは、この54ビットのキー情報KY1を第2のキー情報KY2に変換して出力する。ここでこのデータ変換回路9Cは、このマスタリング装置1により作成するコンパクトディスクの仕様に応じてデータ変換処理の内容が設定され、例えばキー情報KY1をシリアルデータに変換することにより、また仕様に応じて、配列を変更し、変調することにより、第2のキー情報KY2を生成する。なおこの実施の形態では、データ変換回路9Cは、キー情報KY1を単にシリアルデータに変換して出力する。

【0027】暗号化回路15は、第1のキー情報KY1により、デジタルオーディオ信号D1を暗号化して出力する。

【0028】変調回路16は、暗号化回路15より出力されるオーディオデータをコンパクトディスクについて規定されたフォーマットに従ってデータ処理することにより、EFM信号S2を生成する。すなわち変調回路16は、オーディオデータをフレーム単位で区切り、サブ

コードジェネレータ13から供給されるサブコードデータSCを順次割り当ててフレーム構造を形成する。さらに各フレームに誤り訂正符号を付加した後、インターリーブ処理し、さらにEFM変調することによってEFM信号S2を生成する。

【0029】この実施の形態に係るコンパクトディスクの製造工程は、このディスク原盤2を現像した後、さらに電鍍処理することによってマザーディスクを作成し、このマザーディスクを用いてスタンパーを作成する。さらにこのスタンパーを用いた射出成形により、ディスク状基板を形成し、このディスク状基板に反射膜、保護膜を順次作成してコンパクトディスクを作成する。

【0030】これによりこのマスタリング装置1を用いて作成されたコンパクトディスクは、暗号化されたデジタルオーディオ信号D1がビット列の繰り返しにより記録され、この暗号化のキー情報KY1から所定の処理手順により生成されたキー情報KY2がビット幅の変化により記録されるようになっている。

【0031】図3は、このようにして作成されたコンパクトディスクを再生するコンパクトディスクプレイヤーを示すブロック図である。このコンパクトディスクプレイヤー20において、スピンドルモータ21は、サーボ回路22の制御によりコンパクトディスク23を線速度一定の条件により回転駆動する。

【0032】光ピックアップ24は、コンパクトディスク23にレーザービームを照射して得られる戻り光より、この戻り光の光量に応じて信号レベルが変化する再生信号RFを生成する。さらに光ピックアップ24は、サーボ回路22の制御により、コンパクトディスク23の半径方向に可動し、これにより所望のトラックをシークできるようになっている。

【0033】2値化回路25は、この再生信号RFを2値化して2値化信号を生成した後、この2値化信号より再生クロックを生成する。さらに2値化回路25は、この再生クロックを基準にして2値化信号を順次ラッチすることにより、再生信号RFから再生データBDを再生する。

【0034】EFM復調回路26は、この再生データBDをEFM復調して出力する。ECC回路27は、EFM復調回路26の出力データをデインターリーブ処理した後、この出力データに付加された誤り訂正符号により誤り訂正処理して出力する。

【0035】暗号処理回路28は、ECC回路27の出力データを受け、デジタル信号処理プロセッサ(DSP)30より出力されるキー情報KY1により暗号化を解除して出力する。

【0036】デジタルアナログ変換回路(D/A)29は、この暗号処理回路28の出力データをデジタルアナログ変換処理し、これによりアナログ信号によるオーディオ信号SAを出力する。

【0037】このようなオーディオデータの再生系に対して、アナログデジタル変換回路(A/D)31は、再生クロックCKを基準にして再生信号RFをアナログデジタル変換処理し、これによりデジタル再生信号DRFを生成して出力する。

【0038】デジタル信号処理プロセッサ30は、図4に示す処理手順を実行することにより、コンパクトディスク23の再生開始時、フロッピーディスク33により供給される処理手順をロードする。さらにデジタル信号処理プロセッサ30は、この処理手順に従ってキー情報KY1を生成し、このキー情報KY1を暗号処理回路28にセットする。

【0039】ここでこの処理手順は、ビット幅の変化により記録された第2のキー情報KY2を検出する検出手順と、この第2のキー情報KY2よりキー情報KY1を生成するデータ処理手順とにより構成される。

【0040】この検出手順において、デジタル信号処理プロセッサ30は、デジタル再生信号DRFより、再生信号RFの信号レベルを検出してビット幅の変化を検出する。さらにフロッピーディスク33により供給される処理手順に従って、サーボ回路22を制御して、コンパクトディスク23の所望のトラックよりビット幅の変化を検出できるようになっている。

【0041】またデータ処理手順において、デジタル信号処理プロセッサ30は、ビット幅の変化により検出されるデジタル信号を、マスタリング装置1のデータ変換回路9Cに対応した処理により処理できるようになっている。

【0042】デジタル信号処理プロセッサ30は、図4に示す処理手順において、ステップSP1からステップSP2に移り、フロッピーディスク33より処理手順でなるプログラムをロードする。続いてデジタル信号処理プロセッサ30は、ステップSP3に移り、この処理手順に含まれる検出手順に従ってコンパクトディスク23よりキー情報KY2を取得し、さらにこの処理手順に含まれるデータ処理手順によりキー情報KY2からキー情報KY1を生成する。デジタル信号処理プロセッサ30は、続くステップSP4において、このキー情報KY1を暗号処理回路28にセットした後、ステップSP5に移ってこの処理手順を終了する。

【0043】この実施の形態においては、デジタル信号処理プロセッサ30は、ロードしたプログラムにより、この一連の処理のうちのステップSP3及びステップSP4の処理手順を、コンパクトディスク23より得られる再生データのフレーム単位で実行し、これにより記録時に対応した処理によりキー情報KY1を生成する。

【0044】すなわちデジタル信号処理プロセッサ30は、ユーザーの操作に応動してサーボ回路22にシークコマンドを発行した後、シークより得られるディジ

タル再生信号DRFをエンベロープ検波する。さらにこのエンベロープ検波結果を所定のしきい値により2値化し、これによりキー情報KY2を再生する。記録時のデータ変換回路9Cに対応する処理により、さらにこのキー情報KY2をパラレル変換処理し、これによりキー情報KY1を生成する。

【0045】これによりこのコンパクトディスクプレイヤー20では、コンパクトディスク23と対により供給されるフロッピーディスク33の処理プログラムに従ってコンパクトディスク23より再生されるデジタルオーディオ信号の暗号化を解除するようになされ、フロッピーディスク33より供給される処理手順の変更により種々の処理手順によりキー情報KY2の検出手順、キー情報KY2からキー情報KY1を生成するデータ処理手順を変更できるようになされている。

【0046】図1は、マスタリング装置1及びコンパクトディスクプレイヤー20の関係を示す模式図である。コンパクトディスクの製造側40では、コンパクトディスクプレイヤー20で再生可能であるとの条件を満たす範囲で、キー情報KY2の記録位置、如何なるタイムコードとの関係等によりキー情報KY1を生成するかが決定され、これによりコンパクトディスク23の仕様が決定される。

【0047】コンピュータ41は、オペレータの操作により、この決定した仕様により、図2について上述したメモリIC9Bに記録するキー情報KY1を生成する。コンパクトディスクの製造側40では、このキー情報KY1をメモリIC9Bに記録してディスク工場42に供給する。またデータ変換回路9Cのデータ変換処理を記録した情報を、デジタルオーディオ信号を記録したテープカセット43と共に、ディスク工場42に供給する。

【0048】ディスク工場42は、コンパクトディスクの仕様に応じて、マスタリング装置1を選択する。さらにメモリIC9Bをマスタリング装置1にセットし、またデータ変換回路9Cのデータ変換処理をセットし、この条件によりテープカセット43に記録されたデジタルオーディオ信号をディスク原盤2に記録する。さらにこのディスク原盤2よりコンパクトディスク23を作成する。

【0049】またコンピュータ41は、コンパクトディスクプレイヤーにおいて、キー情報KY2を検出する検出手順、この再生したキー情報KY2よりキー情報KY1を作成するデータ処理手順による処理プログラムをフロッピーディスク44に記録する。

【0050】コンパクトディスクの製造側40では、コピー装置45において、このフロッピーディスク44の内容がコピーされて、図3について上述したフロッピーディスク33が作成され、コンパクトディスク23とフロッピーディスク33との組み合わせがユーザーに供給

される。

【0051】以上の構成において、コンパクトディスクの製造側40では(図1)、コンパクトディスク23の仕様が決まると、この決定に従ってコンピュータ41によりデジタルオーディオ信号を暗号化するキー情報KY1が作成され、このキー情報KY1がメモリIC9Bに記録されてディスク工場42に供給される。またコンパクトディスク23に記録するキー情報KY2をキー情報KY1より生成するデータ変換手法が、ディスク工場42に連絡される。

【0052】これに対応してディスク工場42では、このコンパクトディスクの作成にマスタリング装置1が選択され(図2)、さらにマスタリング装置1のキー情報生成回路9にメモリIC9Bがセットされ、データ変換回路9Cのデータ変換処理が連絡されたデータ変換手法にセットされる。

【0053】これによりマスタリング装置1では、デジタルオーディオ信号D1の各フレームのタイムコードによりメモリIC9Bがアクセスされ、このメモリIC9Bに格納されたキー情報KY1によりデジタルオーディオ信号D1が暗号化される。さらにこのデジタルオーディオ信号D1にサブコードデータSC、誤り訂正符号が付加され、EFM変調されてEFM信号S2が生成される。マスタリング装置1では、回転するディスク原盤2にレーザービームL3を照射し、このレーザービームL3がEFM信号S2によりオンオフ制御されることにより、EFM信号S2に応じたピット形状が順次ディスク原盤2に露光される。

【0054】この処理と平行して、マスタリング装置1では、データ変換回路9Cにおいて、コンピュータ41により通知されたデータ変換処理によりキー情報KY1がキー情報KY2にデータ変換処理され、このキー情報KY2に応じてレーザービームL1の光量が切り換えられる。コンパクトディスクの製造工場では(図1)、このようにして露光されたディスク原盤2よりコンパクトディスク23が作成され、これによりピット幅の変化によりキー情報KY2が記録される。

【0055】このようにしてピット幅が変化するように作成されたコンパクトディスク23においては、保護膜、反射膜を剥離してディスク状基板よりスタンパーを作成するコピー方法においては、ピット幅の変化が損なわれ、これにより違法コピーの作成が困難化される。またコンパクトディスクを再生して得られるEFM信号等によりコピーのコンパクトディスクを作成する場合、ピット幅の変化が失われることにより、この種の方法による違法コピーが防止される。

【0056】このようにしてコンパクトディスク23を作成する他方で、コンパクトディスクの製造側40では、コンパクトディスク23に記録したキー情報KY2を検出する検出手順、キー情報KY2よりキー情報KY

1を作成するデータ処理手順がフロッピーディスク33に記録され、このフロッピーディスク33がコピーされ、コンパクトディスク23と組み合わせられて、ユーザーに提供される。

【0057】これにより正規の流通ルートにより流通する正規のコンパクトディスクについては、対応するフロッピーディスク33が組み合わせられることにより、コンパクトディスクより得られるデジタルオーディオ信号を正しく暗号解除することができる。これに対してこのコンパクトディスクの暗号化を解析して作成される違法コピーのコンパクトディスクに対しては、定期的に、キー情報KY2の記録位置、キー情報KY1からキー情報KY2を生成するデータ変換手法、キー情報KY1自体等を変更することにより、実質的に解析困難にすることができる。またこれらの関係でなる暗号化の手法が解析されて違法コピーが作成されたとしても、これらの関係等を変更することにより、フロッピーディスク33により提供される処理手順との対応関係を誤ったものとしてことができ、これにより暗号化されたデジタルオーディオ信号の正しい再生を困難にすることができる。

【0058】すなわちユーザー側においては(図3)、この組み合わせられて提供されたコンパクトディスク23及びフロッピーディスク33がコンパクトディスクプレイヤー20にセットされ、再生開始時、フロッピーディスク33に記録された処理手順がデジタル信号処理プロセッサ30にロードされる。コンパクトディスクプレイヤー20では、このロードされた処理手順の検出手順に従って、再生信号RFがアナログデジタル変換回路31によりデジタル再生信号DRFに変換され、このデジタル再生信号DRFのエンベロープがデジタル信号処理プロセッサ30で検出されてキー情報KY2が検出される。

【0059】さらにロードされた処理手順に含まれるデータ処理手順に従って、このキー情報KY2がパラレルデータでなるキー情報KY1に変換され、このキー情報KY1が順次暗号処理回路28にセットされる。これによりコンパクトディスクプレイヤー20においては、暗号処理回路28において、コンパクトディスク23を再生して得られるデータ列の暗号化が解除され、その結果得られるデジタルオーディオ信号がアナログ信号に変換されて出力される。

【0060】以上の構成によれば、暗号化して記録されたデジタルオーディオ信号を再生する際に、フロッピーディスク33より提供される検出手順に従って、ビット幅により記録されたキー情報KY2を検出し、同様に提供されるデータ処理手順に従ってこのキー情報KY2をキー情報KY1に変換して暗号化を解除することにより、またこの検出手順、データ処理手順を光ディスク以外の外部機器でなるフロッピーディスク33により変更可能に設定したことにより、必要に応じて暗号化の

手順を変更して、これに対応するように検出手順、データ処理手順を変更することができる。これにより必要に応じて暗号化を変更して暗号処理の解析による違法コピーの作成を困難にすることができ、また違法コピーされた場合でも正しい再生を困難にすることができ、これらにより従来に比して一段と確実に違法コピーを防止することができる。

【0061】またビット幅により記録した第2のキー情報KY2を検出することにより、違法にコピーされたコンパクトディスクについては、このビット幅により記録されたキー情報KY2を複製困難にすることができ、これによっても違法コピーを排除することができる。

【0062】なお上述の実施に形態においては、順次変化するサブコードデータに対応して順次キー情報KY1を切り換える場合について述べたが、本発明はこれに限らず、特定のキー情報KY1により暗号化する場合にも広く適用することができる。なおこの場合、図2について上述したマスタリング装置1においては、メモリIC9Bより固定値のキー情報KY1を出力することにより対応することができる。またキー情報KY2については、コンパクトディスク23の特定アドレスについてだけ記録することができ、この場合に他の箇所にはダミーの情報、さらにはキー情報KY1、KY2の検出、データ変換に参考とする一部情報等を記録することもできる。またコンパクトディスクプレイヤー20においては、再生開始時、フロッピーディスク33より供給される処理手順に従って、この特定アドレスを再生してキー情報KY2を検出することにより対応することができる。なおこれらは、上述の実施に形態に対して、ビット幅により記録した第2のデジタル信号の検出手順を変更する関係にある。

【0063】また上述の実施に形態においては、キー情報KY1を単にパラレルデータに変換してキー情報KY2を記録する場合について述べたが、本発明はこれに限らず、パラレルデータに変換した後、配列を変更して記録する場合、種々の変調方式により変調して記録する場合等、種々のデータ変換方式を広く適用することができる。なおこの場合、図2について上述したマスタリング装置1においては、データ変換回路9Cのデータ変換処理を変更することにより対応することができる。またコンパクトディスクプレイヤー20においては、フロッピーディスク33より供給されるデータ処理手順に従って、検出したキー情報KY2をデータ処理することにより対応することができる。なおこれらは、上述の実施に形態に対して、第2のデジタル信号よりキー情報を生成するデータ処理手順を変更する関係にある。

【0064】さらに上述の実施の形態においては、ビット幅の変化によりキー情報KY2でなる第2のデジタル信号を記録する場合について述べたが、本発明はこれに限らず、例えば故意にビット誤りを形成して第2のデ



デジタル信号を記録する場合、ビット長の変位により第2のデジタル信号を記録する場合等にも広く適用することができる。この場合、コンパクトディスクプレイヤーにおいて、これらの何れの方式にも対応できるようにし、フロッピーディスク33より提供される検出手順に従ってこれら何れかの方式により記録された第2のデジタル信号、又はこれらの組み合わせにより記録された第2のデジタル信号を検出することになる。

【0065】また上述の実施の形態においては、コンパクトディスク以外の外部の機器としてフロッピーディスクにより処理手順を提供する場合について述べたが、本発明はこれに限らず、例えばフラッシュメモリなどのメモリチップにより処理手順を提供してもよく、さらには電話回線等の通信回線により提供してもよい。

【0066】さらに上述の実施の形態においては、本発明をコンパクトディスクに適用する場合について述べたが、本発明はこれに限らず、DVD等、種々の光ディスク及び光ディスク再生装置に広く適用することができる。

【0067】

【発明の効果】 上述のように本発明によれば、暗号化の解除に必要なキー情報を光ディスクより検出するのに必要な手順を、光ディスク以外の機器の外部より取得することにより、必要に応じて暗号化手法を変更して、暗号

化の解析を困難にすることができ、また暗号化の解析により違法コピーが作成された場合でも、正しい再生を困難にすることができる。これにより従来に比して一段と確実に違法コピーを防止することができる。

【図面の簡単な説明】

【図1】 本発明の実施の形態に係るコンパクトディスクの製造工程等を示す模式図である。

【図2】 図1の工程に適用されるマスタリング装置を示すブロック図である。

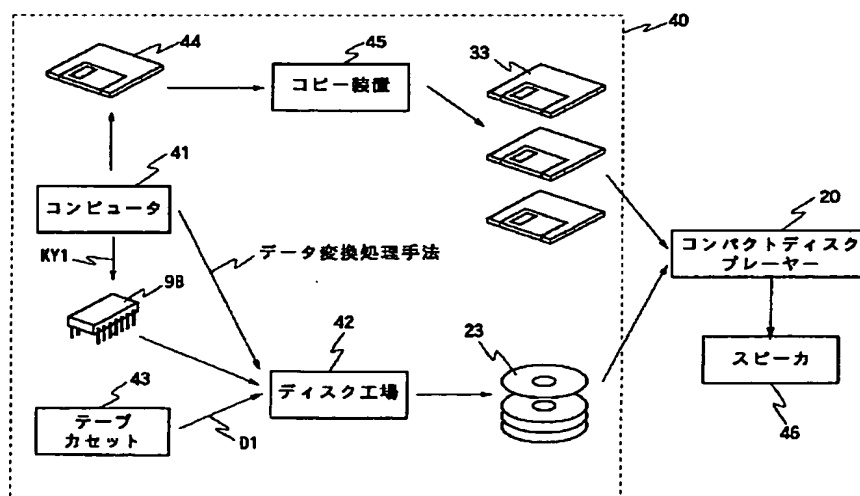
【図3】 図2のマスタリング装置により作成されたコンパクトディスクの再生に使用されるコンパクトディスクプレイヤーを示すブロック図である。

【図4】 図3のコンパクトディスクプレイヤーにおけるデジタル信号処理プロセッサの処理手順を示すフローチャートである。

【符号の説明】

1……マスタリング装置、2……ディスク原盤、9……キー情報生成回路、9A……アドレスデコーダ、9B……メモリIC、9C……データ変換回路、20……コンパクトディスクプレイヤー、23……コンパクトディスク、31……アナログデジタル変換回路、30……デジタル信号処理プロセッサ、33、44……フロッピーディスク

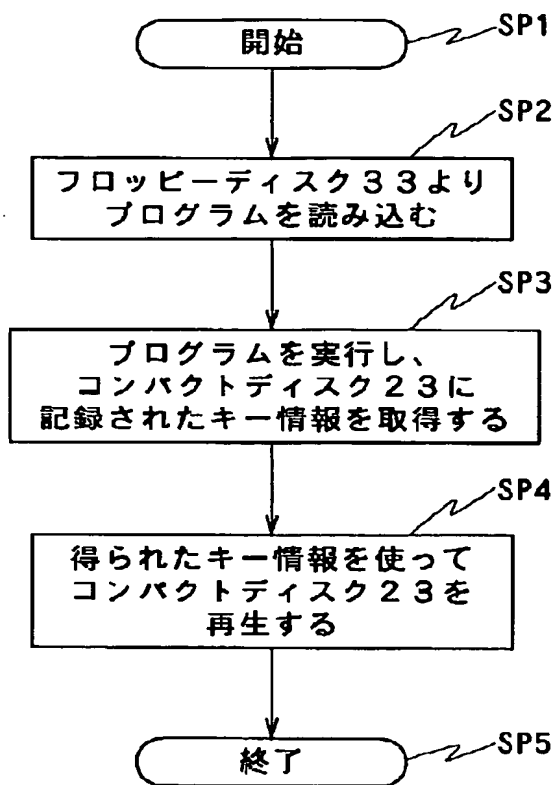
【図1】



[illegible]

20: コンパクトディスクプレイヤー

【図4】



# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-187013

(43)Date of publication of application : 09.07.1999

(51)Int.Cl.

H04L 9/08  
G09C 1/00

(21)Application number : 09-354401

(71)Applicant : IBM JAPAN LTD

(22)Date of filing : 24.12.1997

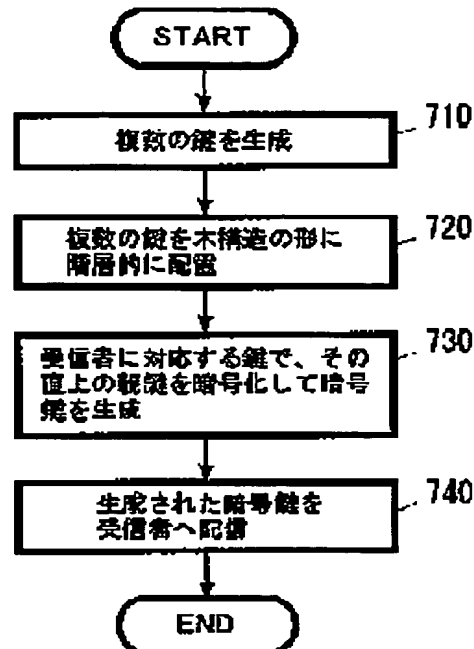
(72)Inventor : MARUYAMA HIROSHI  
TOKUYAMA TAKESHI  
URAMOTO NAOHIKO

## (54) CRYPTOGRAPHIC KEY DISTRIBUTION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method and a system for minimizing procedures required for updating a cryptographic key by structuring the cryptographic key into tree structure.

SOLUTION: First of all, plural keys more than the number of recipients are generated 710, and the plural keys are hierarchically arranged 720 in the form of tree structure. Next, the plural recipients are made correspondent to the keys hierarchically arranged in the form of tree structure, and the cryptographic keys of the respective recipients are generated as a key stream having keys from the root of tree structure to positions corresponding to the said recipients in the tree structure. Thus, after the cryptographic key is generated 730, the generated cryptographic key is distributed 740 to the correspondent recipient.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]